CLAIMS

What is claimed is:

1	1. A method for securing communications between a first device and a		
2	second device, the method comprising:		
3	mutually authenticating the first device and the second device;		
4	generating an integrity check value by the first device; and		
5	sending the integrity check value with a message from the first device to the		
6	second device.		
1	2. The method of claim 1, wherein the generating of the integrity check value		
2	comprises:		
3	extracting a selected number of bits from a pseudo-random data stream for use as		
4	coefficients of a matrix having M rows and N columns; and		
5	performing operations on both contents of the message and the coefficients of the		
6	matrix to generate the integrity check value.		
1	3. The method of claim 2, wherein prior to extracting the selected number of		
2	bits from the pseudo-random data stream, the method comprises:		
3	inputting keying material into a cipher engine performing operations in		
4	accordance with a predetermined stream cipher; and		
5	producing the pseudo-random data stream by the cipher engine.		
1	4. The method of claim 3, wherein the predetermined stream cipher is Data		
2 ·	Encryption Standard in counter mode.		

1	5.	The method of claim 2, wherein the extracting of the selected number of		
2	bits includes			
3	assign	ning M bits from the selected number of bits as a first column of the matrix;		
4	and			
5	reiter	atively assigning M unique bits from a remainder of the selected number of		
6	bits for each	remaining column of the matrix.		
1	6.	The method-of claim 5, wherein the performing of the operations includes		
2	perfo	rming arithmetic operations on M bits from the content of the message and		
3	correspondin	ng coefficients of the first column of the matrix to produce a first plurality of		
4	resultant values; and			
5	perfo	rming exclusive OR operations between each of the first plurality of		
6	resultant val	ues to produce a bit of the integrity check value.		
1	7.	The method of claim 6, wherein the arithmetic operations are bitwise		
2	multiplication	on operations.		
1	8.	The method of claim of claim 6, wherein the performing of the operations		
2	further inclu	des		
3	perfo	orming arithmetic operations on the M bits from the content of the message		
4	with corresponding coefficients for a remaining N-1 columns of the matrix to produce a			
5	second plurality of resultant values associated with each of the remaining N-1 columns;			
6	and ·			
7	perfo	orming exclusive OR operations between resultant values associated with		
8	each remain	ing N-1 column of the matrix to produce N-1 bits of the integrity check value.		

1	7. The method of claim 2, wherein the extracting of the selected number of		
2	bits includes		
3	assigning M bits from the selected number of bits as a first column of the matrix;		
4	and		
5	reiteratively reassigning the M bits in accordance with a predetermined bit		
6	rotation for columns of the matrix excluding the first column.		
1	10. The method of claim 9, wherein the performing of the operations includes		
2	multiplying M bits from the content of the message with corresponding		
3	coefficients of the N columns of the matrix to produce a plurality of resultant values		
4	associated with each coefficient of the matrix; and		
5	performing exclusive OR operations on the plurality of resultant values along the		
6	N columns of the matrix to produce N bits of the integrity check value.		
1	11. The method of claim 10, wherein the performing of the operations further		
2	includes:		
3	reiteratively computing the integrity check value based on successive groups of		
4	bits of the message.		
1	12. A method comprising:		
2	computing an integrity check value for an incoming message; and		
3	determining whether the incoming message is valid by comparing the computed		
4	integrity check value with a recovered integrity check value accompanying the incoming		
5	message		

1	13. The method of claim 12, wherein prior to computing the integrity check		
2	value, the method further comprises decrypting the incoming message.		
	· · · · · · · · · · · · · · · · · · ·		
1	14. The method of claim 13, wherein the decrypting of the incoming message		
2	includes		
3	producing a pseudo-random data stream;		
4	extracting a predetermined number of bits from the pseudo-random data stream;		
5	and .		
6	exclusively OR'ing portions of the incoming message with the predetermined		
7	number of bits from the pseudo-random data stream.		
.1	15. The method of claim 12, wherein the computing of the integrity check		
2	value includes		
3	producing a pseudo-random data stream;		
4	extracting a selected number of bits from the pseudo-random data stream to		
5	generate a matrix having M rows and N columns where M and N are positive whole		
6	numbers;		
7	multiplying M bit values of the message with corresponding coefficients of the N		
8.	columns of the matrix to produce a plurality of resultant values; and		
9	performing exclusive OR operations between resultant values associated with		
10	each column of the matrix to produce N bits of the integrity check value.		
1	16. The method of claim 14, wherein the computing of the integrity check		

extracting a selected number of bits from the pseudo-random data stream to

value includes

generate a matrix having M rows and N columns;

2

3

5	multiplying M bit values of a first group of bits of the message with		
6	corresponding coefficients of the N columns of the matrix to produce a plurality of		
7	resultant values associated with each of the coefficients; and		
8	performing exclusive OR operations between resultant values associated with		
9	each of the N columns of the matrix to produce N bits of the integrity check value.		
1	17. The method of claim 16, wherein the bits associated with the selected		
2	number of bits differ from the bits associated with the predetermined number of bits.		
	10		
1	18. An electronic system comprising:		
2	a first device to generate an integrity check value and transmit the integrity check		
3	value along with a message; and		
4	a second device to determine whether the message has been altered by comparing		
5	a newly generated integrity check value with the integrity check value recovered with the		
6	message.		
1	19. The electronic system of claim 18, wherein the first device is a processor		
2	and the second device is a memory.		
1	20. The electronic system of claim 18, wherein the first device includes an		
2	integrity check value (ICV) generator to produce an integrity check value based on a		
3	selected group of bits from a pseudo-random data stream and contents of the message.		
1	21. A program loaded in internal memory for execution by a processor of an		
2	electronic system, the program comprising:		
3	code for authenticating both the first device and the second device;		
4	code for generating an integrity check value by the first device; and		

- 5 code for sending the integrity check value with a message from the first device to
- 6 the second device.